US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

November 7, 2008
Volume 3, Issue 4

QUARTERLY TRENDS AND ANALYSIS REPORT

www.us-cert.gov

Introduction

This report summarizes and provides analysis of incident reports submitted to US-CERT during the U.S. Government fiscal year 2008 fourth quarter (FY08 Q4), which is the period of July 1, 2008 to September 30, 2008.

US-CERT is a partnership between the Department of Homeland Security (DHS) and the public and private sectors. Established in 2003 to protect the nation's internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the nation. The organization interacts with federal agencies, state and local governments, industry professionals, and others to improve information sharing and incident response coordination and to reduce cyber threats and vulnerabilities.

US-CERT provides the following support:

- 24 x 7 x 365 triage support to federal, public, and private sectors, and the international community
- cyber security event monitoring and predictive analysis
- advanced warning on emerging threats
- incident response capabilities for federal and state agencies
- malware analysis and recovery support
- trends and analysis reporting tools
- development and participation in national and international level exercises

INSIDE THIS ISSUE

The purpose of this report is to provide awareness of the cyber security trends as observed by US-CERT. The analysis in this report is based on incident information that has been reported to US-CERT, incidents identified by US-CERT, and public/private sector information identified when correlating and analyzing the data. A computer incident within US-CERT is, as defined by NIST Special Publication 800-61, a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices.

This report also provides information on notable security topics and trends, including emerging threats and updates to topics discussed in previous issues.

Cyber Security Trends, Metrics, and Security Indicators

US-CERT interacts with federal agencies, industry, the research community, state and local governments, and others to collect reasoned and actionable cyber security information and to identify emerging cyber security threats. Based on the information reported, US-CERT was able to identify the following cyber security trends for fiscal year 2008 fourth quarter (FY08 Q4).

The definition of each reporting category is delineated in Table 1 shown below.

Category	Description
CAT 1 Unauthorized Access	In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource.
CAT 2 Denial of Service (DoS)	An attack that *successfully* prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.
CAT 3 Malicious Code	*Successful* installation of malicious software (e.g., virus, worm, spyware, bot, Trojan horse, or other code-based malicious entity that infects or affects an operating system or application). Agencies are *not* required to report malicious logic that has been *successfully quarantined* by antivirus (AV) software.
CAT 4 Improper Usage	A person violates acceptable computing use policies.
CAT 5 Scans, Probes, or Attempted Access	Any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.
CAT 6 Investigation	*Unconfirmed* incidents of potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.

Figure 1 displays the overall distribution of cyber security incidents and events across the six major categories described in Table 1.

The proportion of Category 5 reports decreased by 3.5% compared to the previous quarter.

Figure 1: Incidents and Events by Category

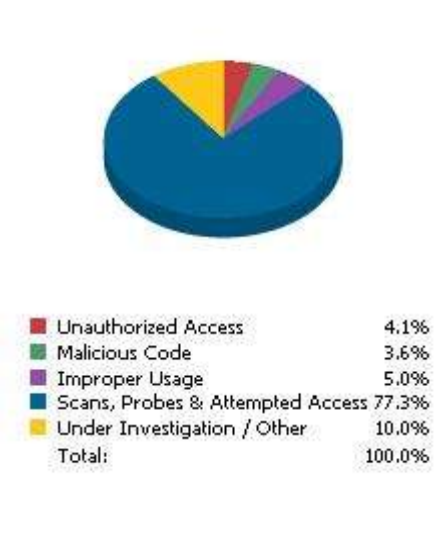

Figure 2 is a breakdown of the top five incidents and events versus all others. The top incident type reported to US-CERT was phishing, accounting for 71.8% of all incidents reported. This is, however, a proportional decrease of 4.5% from the previous quarter.

US-CERT encourages all users and organizations to report any activities that you feel meet the criteria for an incident. To learn more about incidents, visit https://forms.us-cert.gov/report/. To report phishing, visit http://www.us-cert.gov/nav/report_phishing.html.

Figure 2: Top Five Incidents vs. All Others

Multimedia Player Vulnerabilities

A number of vulnerabilities in multimedia players and plug-ins allowed remote attackers to potentially execute arbitrary code or perform other malicious activity on vulnerable systems. Widely used multimedia applications such as Adobe Flash, Apple QuickTime, RealNetworks RealPlayer, and Microsoft (MS) Windows Media Player all were found to contain critical vulnerabilities throughout FY08.

Adobe Flash
Critical vulnerabilities in Adobe Flash Player during FY08 were exploited to allow attackers to take control of vulnerable systems via specially crafted SWF media. If a user opened such files, an attacker could execute arbitrary code, perform DNS rebinding or cross-site scripting attacks, conduct port scans, or cause a denial of service.

During the fourth quarter, US-CERT posted a Current Activity entry to warn users of malware involving a fraudulent Flash Player installer. Adobe warned in a security bulletin that the worm spreads via fraudulent posts on social networking sites, which included links to fake sites that prompted users to update their versions of Flash Player. If users attempted to use the installer to make the update, malware could be downloaded and installed onto their systems.

In September 2008, news reports warned "a bug in Flash has been used for more than a month by attackers to poison Macintosh and Windows users' clipboards with URLs to malicious sites."[1] If users pasted the URL into the address bar of their web browsers, they would be taken to a site selling bogus software.

Apple QuickTime
During FY08, multiple vulnerabilities in Apple QuickTime and its associated plug-ins had been exploited, which impacted multiple Mac OS X and MS Windows operating systems. Several patches were released by Apple to address these vulnerabilities throughout the fiscal year, from versions 7.3 to 7.5.5. QuickTime version 7.5.5 was released during the fourth quarter to address nine vulnerabilities. The method in which previous versions of QuickTime processed certain movie and picture file types could allow an attacker to terminate applications or execute arbitrary code.

US-CERT released Vulnerability Note VU#659761 in FY08 Q1, Technical Cyber Security Alert TA08-162C and Cyber Security Alert SA08-162C in the fourth quarter, and multiple Current Activity entries throughout FY08.

Windows Media Player
During FY08, multiple critical vulnerabilities in Microsoft Windows Media Player were identified and patched. Specially crafted video or audio files could be used by remote attackers to execute arbitrary code or other malicious activity on vulnerable systems. US-CERT alerted users to implement security updates throughout the year via the National Cyber Alert System and Current Activity entries regarding Microsoft Security Bulletins.

Phishing and Spamming Trends

Several wide-scale phishing campaigns were noted during FY08 Q4:

- Leading up to the Olympics in August 2008, there was an increase of public reports that indicated malware was spreading via spam messages related to the Olympics and to fake CNN news reports referring to the Olympics and to earthquakes in China. If users clicked on the link to one of these fake news reports, they would be prompted to install a Flash Player update. If users attempted to install the update, malware could be downloaded and installed onto their systems.[2]

- Public reports indicated a phishing attack circulating via email messages that appeared to be targeting Apple MobileMe users. These messages claimed that there was a problem with the user's billing information and instructed the user to follow a web link to update personal information. Clicking on this link directed the user to a web page that contained a seemingly legitimate web form requesting personal and financial information. Any information entered in this form is not sent to Apple but rather to a malicious attacker.[3]

- US-CERT became aware of public reports of an attack circulating via bogus email messages that

[1] http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9115269&source=rss_topic17

[2] http://www.us-cert.gov/current/archive/2008/08/12/archive.html#rise_in_spam_messages_circulating

[3] http://www.us-cert.gov/current/archive/2008/08/22/archive.html#apple_mobileme_phishing_scam

claimed to be from "US Customs Service." The messages contained a subject line such as "Parcel requires declaration" and indicated that a parcel received was addressed to the recipient of the email. Some of these messages also encouraged users to open an attachment to the message that could contain malicious code.[4]

- A phishing campaign based on bogus e-tickets used email messages that appeared to be from legitimate airlines. These email messages instructed users to open the attachment to obtain the e-ticket. If a user opened this attachment, a file could be executed to infect the user's system with malicious code.[5]

DNS Cache Poisoning

DNS servers employ caches of memory to improve their performance when answering multiple identical queries. When a DNS server answers a query with information that did not originate from an authoritative DNS server, it is considered poisoned. DNS cache poisoning (sometimes referred to as cache pollution) is an attack technique that allows an attacker to introduce forged DNS information into the cache of a caching nameserver. Due to the caching mechanism, a poisoned DNS server will continue to answer queries for the forged information until the cached answer times out. A successful attack could result in a nameserver's clients being redirected to an improper and possibly malicious host. The patches released on July 8th used source port randomization to mitigate the risk.

The U.S. National Institute of Standards and Technology (NIST) Special Publication 800-81 "Secure Domain Name System (DNS) Deployment Guide" contains detailed information about the secure deployment of DNS servers.

US-CERT released several products on the public website (http://www.us-cert.gov). These products included Technical Cyber Security Alert TA08-190B, a Current Activity entry, and a Vulnerability Note VU#800133 that lists vendors that released DNS patches.

[4] http://www.us-cert.gov/current/archive/2008/08/05/archive.html#u_s_customs_and_border

[5] http://www.us-cert.gov/current/archive/2008/08/05/archive.html#airline_e_ticket_email_attack

National Cyber Alert System

Stay informed and involved by subscribing to the products included in the US-CERT National Cyber Alert System (NCAS). There are five products available for various technical levels and needs. They are as follows:

Current Activity – Notifies users of the most frequent, high-impact types of security incidents currently reported to US-CERT.

Technical Cyber Security Alerts – Provide timely information about current security issues, vulnerabilities, and exploits.

Cyber Security Bulletins – Summarize information that has been published about new vulnerabilities.

Cyber Security Alerts – Alert non-technical readers to security issues that affect the general public.

Cyber Security Tips – Provide information and advice for non-technical readers about a variety of common security topics.

Visit http://www.us-cert.gov/cas/signup.html to learn more

Contacting US-CERT

If you would like to contact US-CERT to ask a question, submit an incident, provide a tip of suspicious activity, or just learn more about cyber security, please use one of the below methods.

If you would like to provide feedback on this report, or if you have comments or suggestions for future reports, please email info@us-cert.gov.

Web Site Address:	http://www.us-cert.gov
Email Address:	info@us-cert.gov
Phone Number:	+1 (888) 282-0870
PGP Key ID:	CF5B48C2
PGP Key Fingerprint:	01F1 9C58 0817 D612 45ED 3FCF 3004 FE8C CF5B 48C2
PGP Key:	https://www.us-cert.gov/pgp/info.asc

Disclaimer

The purpose of the analysis within this report is to provide awareness and information on cyber threats as seen and reported to US-CERT. The content of this report was developed with the best information available at the time of analysis; if further information becomes available, US-CERT may publish it in a future report.